What is Claimed is:

1. A method for using multi-layer identity-based encryption (IBE) to securely convey a message containing message data over a communications network from a sender to a recipient, comprising:

at the sender, encrypting the message using at least two layers of IBE encryption by using an inner layer of message encryption having an associated inner-layer IBE public key to encrypt the message data and by using an outer layer of message encryption having an associated outer-layer IBE public key to encrypt the inner-layer IBE public key;

sending the encrypted message to the recipient; and

at the recipient, decrypting the encrypted message using an outer-layer IBE private key corresponding to the outer-layer IBE public key and using an inner-layer IBE private key corresponding to the inner layer IBE public key.

2. The method defined in claim 1 wherein using the outer layer of message encryption to encrypt the inner-layer IBE public key comprises encrypting the inner-layer IBE public key with the outer-layer IBE public key without using a symmetric key.

3. The method defined in claim 1 wherein using the outer layer of message encryption to encrypt the inner-layer IBE public key comprises encrypting the inner-layer IBE public key with a symmetric key and encrypting the symmetric key with the outer-layer IBE

public key.

4. The method defined in claim 3 wherein sending the encrypted message to the recipient comprises sending the encrypted inner-layer IBE public key to the recipient with the encrypted message, and wherein decrypting the encrypted message at the recipient further comprises using the outer-layer IBE private key to decrypt the encrypted inner-layer IBE public key to produce an unencrypted version of the inner-layer IBE public key at the recipient.

5. The method defined in claim 1 wherein encrypting the message comprises encrypting the message using at least three layers of IBE encryption and wherein the outer layer is not an outermost layer.

6. The method defined in claim 1 wherein encrypting the message comprises encrypting the message using a symmetric key.

7. The method defined in claim 6 wherein encrypting the message comprises encrypting the message data using the symmetric key and encrypting the symmetric key using the inner-layer IBE public key.

8. The method defined in claim 7 wherein encrypting the message further comprises encrypting the inner-layer IBE public key using the outer-layer IBE public key.

9. The method defined in claim 8 wherein the message data that has been encrypted using the symmetric key and the inner layer IBE public key that has been encrypted using the outer-layer IBE public key are sent to the recipient with the message and wherein decrypting the message at the recipient comprises:

using the outer-layer IBE private key to decrypt the inner-layer IBE public key that has been encrypted using the outer-layer IBE public key;

using inner-layer IBE private key to decrypt the symmetric key that has been encrypted using the inner-layer IBE public key; and

using the symmetric key that has been decrypted using the inner-layer IBE private key to decrypt the message data that was encrypted using the symmetric key.

10. The method defined in claim 1 wherein the outer-layer IBE public key is less sensitive than the inner-layer IBE public key and wherein encrypting the message comprises using the less-sensitive outer-layer IBE public key to encrypt the more-sensitive inner-layer IBE public key to conceal the more-sensitive inner-layer IBE public key during transmission from the sender to the recipient.

11. The method defined in claim 10 wherein encrypting the message comprises encrypting the message using at least three layers of IBE encryption and wherein the outer layer is not an outermost layer.

12. The method defined in claim 1 wherein the message data is provided in an XML data structure containing data attributes of the message data, the method further comprising using at least some of the data attributes in forming the inner-layer IBE public key and the outer-layer IBE public key.

13. The method defined in claim 12 wherein at least one of the data attributes has an associated sensitivity level and wherein encrypting the message data comprises using the sensitivity level in determining how to encrypt the message.

14. The method defined in claim 13 further comprising:

at the sender, obtaining information on the associated sensitivity level in the form of an XML record.

15. The method defined in claim 1 wherein the message comprises content having an age-based access policy criteria and wherein encrypting the message comprises using the age-based access criteria as at least part of the inner-layer IBE public key.

16. The method defined in claim 1 wherein encrypting the message comprises encrypting an email message.

17. The method defined in claim 1 wherein encrypting the message comprises encrypting an instant

message.

18. The method defined in claim 1 wherein the inner-layer IBE public key and the outer-layer IBE public key have overlapping components and wherein encrypting the message comprises encrypting the inner layer of the message using the inner-layer IBE public key that has overlapping components.

19. The method defined in claim 1 wherein encrypting the message further comprises using an additional-layer IBE public key to perform an additional layer of IBE encryption on the message, wherein the additional-layer IBE public key is less sensitive than the outer-layer IBE public key and is used to encrypt the outer-layer IBE public key.

20. The method defined in claim 19 wherein the inner-layer IBE public key, the outer-layer IBE public key, and the additional-layer IBE public key each have corresponding IBE public key components and wherein each IBE public key component in the additional-layer IBE public key is contained in the outer-layer IBE public key and wherein each IBE public key component in the outer-layer IBE public key is contained in the inner-layer IBE public key.

21. A method for using identity-based-encryption (IBE) to securely convey a message having message data M from a sender to a recipient over a communications network, comprising:

encrypting the message by performing at least an inner layer of IBE encryption and an outer layer of IBE encryption at the sender, wherein:

performing the inner layer of IBE encryption includes encrypting the message data M using a symmetric key S to produce encrypted message data M_S and encrypting the symmetric key S using an IBE public key QG associated with the inner layer of IBE encryption to produce an IBE-encrypted symmetric message key S_{QG}, and

performing the outer layer of IBE encryption includes encrypting at least the IBE public key QG using an IBE public key QL, wherein the IBE public key QL is less sensitive than the IBE public key QG; and

sending at least the encrypted message data M_S, the IBE-encrypted symmetric message key S_{QG}, and the encrypted IBE public key QG to the recipient.

22. The method defined in claim 21 further comprising sending the IBE public key QL to the recipient.

23. The method defined in claim 21 wherein:

performing the outer layer of IBE encryption comprises encrypting the IBE public key QG using the IBE public key QL to produce an IBE-encrypted public key QG_{QL}; and

sending the encrypted IBE public key QG to the recipient comprises sending QG_{QL} to the recipient.

24. The method defined in claim 21 wherein a symmetric key S' is used in performing the outer layer of IBE encryption by encrypting the IBE public key QG using the symmetric key S' to produce $QG_{S'}$.

25. The method defined in claim 24 wherein performing the outer layer of IBE encryption comprises encrypting the symmetric key S' with the IBE public key QL to produce an IBE-encrypted symmetric key S'_{QL}.

26. The method defined in claim 25 wherein sending the encrypted IBE public key QG to the recipient comprises sending $QG_{S'}$ and S'_{QL} to the recipient.

27. The method defined in claim 21 wherein the recipient has an identity and wherein the IBE public key QL is based on the recipient's identity, the method further comprising performing the outer layer of IBE encryption using the IBE public key QL that is based on the recipient's identity.

28. The method defined in claim 21 wherein the recipient has an email address and wherein the IBE public key QL is based on the recipient's email address, the method further comprising performing the outer layer of IBE encryption using the IBE public key QL that is based on the recipient's email address.